Bild: © New Africa/shutterstock.com

GOLFCLUBS – LUKRATIVES ZIEL FÜR CYBER-KRIMINELLE

Wenn Kundendaten zum Angriffsziel werden

Die zunehmende Digitalisierung sorgt unausweichlich für mehr Daten auf den Servern der Golfanlagen. Zahlreichere Bilder der Anlage, Events oder Sponsoren bzw. die vielen Listen, Statistiken, Auswertungen oder Dokumente – alles wird gespeichert.

Viele Anlagen haben zwischenzeitlich begonnen, kundenrelevante Dokumente und Daten in einem CRM-System (Customer Relationship Management) zu verwalten, um auf die Informationen schnell und komfortabel zugreifen zu können. Die Verfügbarkeit der IT-Systeme spielt im Golfsport eine immer größere Rolle, daher muss sich das Management der Anlagen mit einem (nicht gerne) denkbaren Szenario beschäftigen: Was wäre, wenn durch einen Datenverlust plötzlich alle Informationen und Systeme nicht mehr zur Verfügung stehen?

„Desaster Recovery" – gibt es einen Notfallplan?

Was tun Sie, wenn Ihre IT-Systeme nicht mehr verfügbar sind? Haben Sie zusammen mit ihrem IT-Verantwortlichen einen Plan, wie Sie sicherstellen, dass die Daten im Fall der Fälle wieder verfügbar gemacht werden können? Spätestens mit der Einführung der DSGVO sind Sie im Rahmen der vorgeschriebenen technischen und organisatorischen Maßnahmen[1] dazu verpflichtet, sich mit diesem Szenario zu beschäftigen und schriftlich zu fixieren, welche Maßnahmen Sie bzw. Ihr IT-Dienstleister unternommen haben, um einen Verlust der Daten bzw. einen nicht berechtigten Zugriff auf die Daten auszuschließen.

Bei der Planung von notwendigen Maßnahmen stellt sich bei den entstehenden Kosten immer eine Frage: Was kostet mich eine Stunde/Tag Ausfall des Systems – und wie lange kann ich so einen Ausfall verkraften? Reicht es also, bei einem Ausfall des Systems am Freitag um 19 Uhr, wenn der Techniker am Montagmorgen erscheint? Je nach Antwort braucht man also Lösungsansätze, die zumindest ein Basissystem möglichst schnell wieder zur Verfügung stellen. Die klassischen Sicherungsmethoden kommen bei der immer komplexer werdenden Anzahl von Angriffen

1 Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO

immer mehr an ihre Grenzen, so dass ein Konzept unter Berücksichtigung aktueller Cyberbedrohungen wichtig ist.

Moderne Malware bringt Anti-Viren-Lösungen an ihre Grenzen

Ein „klassischer" Virenscanner basiert darauf, dass mehrmals täglich sog. „Signatur-Informationen" vom Hersteller der Virenschutzsoftware aktualisiert werden. Der Virenscanner kann dann aufgerufene Prozesse mit diesen Signaturen vergleichen und ggf. stoppen, wenn diese als bösartig eingestuft werden. Genau an dieser Stelle setzen die Kriminellen an: Zum einen wird verstärkt versucht, sog. „Zero-Day-Attacken" (Angriffe auf fehlerhaften Programmcode, noch bevor der Hersteller den Fehler beheben konnte) durchzuführen oder die Malware so häufig zu verändern, dass die Signaturen mit der Aktualisierung der Beschreibungen nicht mithalten können.

Moderne Lösungen setzen dabei auf einen anderen Ansatz: Sie beobachten das Verhalten einer Anwendung und verhindern deren Ausführung, wenn diese sich unangemessen verhält. Diese Methode nennt man NGAV (Next Generation Anti Virus). Vorteil dieser Methode ist vor allem, dass es keiner aktualisierten Signaturen bedarf und auch der Ressourcenverbrauch dieser Lösungen auf dem Computer sehr viel geringer als beim Vergleich mit Millionen von Signaturen ist. Zusammen mit einer dauerhaften Verhaltensüberwachung kurz EDR (Endpoint Detection und Response) kann so ein unberechtigter Zugriff auf Dateien und Netzwerk unterbunden werden. Für alle PC CADDIE://online-Cloud bzw. Netwatch-Kunden ist z.B. das Tool „FortiEDR"[2] auf allen betreuten Servern im Einsatz, das diese beiden Technologien miteinander kombiniert.

Cybercrime im Golfbusiness?

Welcher Schaden durch einen Datenverlust entstehen kann, lesen wir immer häufiger in der Presse:

- Eines der größten Industrieunternehmen in Österreich hat 4 Millionen Euro an Lösegeld bezahlt, um die Funktionalität der IT-Systeme wiederherzustellen, weil dies aus den bestehenden Sicherungen nicht möglich war und der abzusehende Schaden noch viel größer eingeschätzt wurde.[3]

- Der Landkreis Anhalt-Bitterfeld ist auch einige Wochen nach einem Verschlüsselungsangriff noch immer nicht in der Lage, seine Systeme in vollem Umfang wieder in Betrieb zu nehmen.[4]

- Durch einen Angriff auf den Softwarehersteller Kaseya haben Kriminelle ihre Verschlüsselungstools bei mehr als 1.500 Unternehmen schnell und wirkungsvoll verteilen können. Die Forderungen der Erpresser für einen „Generalschlüssel" lagen am Anfang bei 60 Millionen Euro[5].

Axel Heck
Geschäftsführer PC CADDIE://online

Auch einige Golfanlagen wurden in den letzten Monaten Opfer solcher Attacken aus dem Internet. Dabei wurden entweder die vorhandenen Daten verschlüsselt oder personenbezogene Daten (z.B. Mitgliederinformationen) gestohlen und mit der Veröffentlichung der Daten gedroht. Problematisch wird eine Verschlüsselung der Daten immer dann, wenn über einen längeren Zeitraum keine aktuelle Datensicherung verfügbar ist. Stellen Sie sich z.B. ein Kundenkonto vor, auf dem Ihre Mitglieder und Gäste Leistungen der Golfanlage konsumieren können (Restaurant, Ballautomaten, Shop etc.). Schon nach wenigen Tagen ist die Chance alle Buchungen zu rekonstruieren und somit den richtigen Kontostand der Kunden wiederherzustellen, fast unmöglich.

2 Schutz und Response-Maßnahmen für Endgeräte mit FortiEDR von Fortinet

3 https://futurezone.at/amp/b2b/ransomware-oesterreichische-firma-zahlte-4-millionen-loesegeld/400699662

4 Hackerangriff: Erste Cyber-Katastrophenfall in Deutschland (handelsblatt.com)

5 Kaseya-Ransomware-Angriff: Rund 1500 Unternehmen betroffen | ZDNet.de

Kommt es zu einer Erpressung, sind die Forderungen der Kriminellen auf den ersten Blick zwar schmerzhaft, aber im Vergleich zum ggf. entstehenden Schaden noch überschaubar (beim Crypto-Trojaner SODIBIKI lag diese z.B. bei 7.500 Euro). Das Problem ist jedoch, dass mit der Zahlung dieser Forderung (natürlich anonym in Bitcoin) der Erpresser auf das Interesse an den verschlüsselten Daten hingewiesen wird. So erhält man dann auch gerne einmal nach der geleisteten Zahlung über die geforderte Summe den Hinweis, dass die Anzahlung eingegangen sei und man nun gerne nochmals einen hohen fünfstelligen Betrag nachzahlen darf, damit die Entschlüsselung auch stattfinden kann. Eine Chance auf die Rückabwicklung der Zahlung oder eine Nachverfolgung gibt es nicht, daher empfehlen alle Sicherheitsexperten und das Bundeskriminalamt von der Zahlung – egal welcher Summe – einer Lösegeldsumme abzusehen. Dass diese Art von Business funktioniert, zeigen die geschätzten Zahlen von gezahltem Lösegeld, das sich im dreistelligen Millionenbereich befindet. Wie viele dieser Zahlungen „erfolgreich" in einer Entschlüsselung endeten, weiß dabei niemand.

Fünf Tipps für den „Fall der Fälle" (Verdacht auf Cyberangriff)

Trennen Sie Ihr Netzwerk vom Internet und auch die einzelnen Rechner/Server vom Netzwerk, um eine weitere Verbreitung des „Schädlings" zu vermeiden.

Nehmen Sie eine Analyse des Angriffs und der entstandenen Schäden zusammen mit Ihrem zuständigen IT-Experten vor und ermitteln Sie auch, ob ggf. personenbezogene Daten von dem Vorfall betroffen sein können.

Informieren Sie Ihren zuständigen Datenschutzbeauftragten schnellstmöglich über den Vorfall, so dass dieser die eventuell notwendigen Meldungen an die Datenschutzbehörden bzw. die Betroffenen Kunden in den vorgegebenen gesetzlichen Fristen erledigen kann.

Prüfen Sie vorhandene Sicherungen vor einem Zurückspielen, denn ggf. befindet sich auch dort schon ein Schadcode, der dann wieder aktiv werden könnte.

Zahlen Sie kein Lösegeld an Cyberkriminelle – auch wenn es ob der ggf. verlorenen Daten „wirtschaftlich sinnvoll" erscheint. Informieren Sie die zuständige Kriminalpolizei über den Vorfall, sofern hier ein krimineller Hintergrund vermutet wird.

Backup – Am besten ohne Risikofaktor Mensch

Eine Sicherung in mehreren Generationen[6] inkl. Auslagerung an einen externen Ort galt in der Vergangenheit als eine „sichere Sache". Während eine räumliche Trennung der Sicherung (z.B. in einem anderen Gebäude) in vielen Golfanlagen machbar ist, bleibt das Thema der Auslagerung der Daten. Einige Golfanlagen tragen die Sicherungsmedien im täglichen, wöchentlichen oder monatlichen Rhythmus in einen Tresor einer Bank oder mit nach Hause zu einem Mitarbeiter aus dem Sekretariat (was der Datenschutzbeauftragte dann nicht so gerne sieht). Das „Problem" einer solchen Sicherung ist immer, die Validierung der Sicherung. Wer ist sicher, dass das Medium, das im Tresor der Bank liegt, im Fall der Fälle auch wirklich verwertbare Daten für die Rücksicherung enthält. Uns ist der Fall einer Golfanlage in der Schweiz bekannt, in der die Mitarbeiter Woche für Woche ein Sicherungsmedium in den Banktresor getragen haben und erst nach 14 Monaten fiel auf, dass der Sicherungsdienst, der die Daten täglich auf das Medium kopieren sollte, nach einem Windows-Update gar nicht mehr gestartet werden konnte. Auf manch anderen Anlagen klappt zwar die Sicherung auf ein externes Medium, aber irgendwie vergessen die Mitarbeiter dann doch dieses Medium „in Sicherheit" zu bringen. Auf den „Faktor Mensch" sollte bei dieser wichtigen Aufgabe möglichst verzichtet werden.

Daher ist heutzutage eine sog. Hybriden-Datensicherung anzuraten. Diese besteht aus einer lokalen Sicherung (am besten auch in einem getrennten Gebäude), um im Fall der Fälle schnell eine Rücksicherung der Daten durchführen zu können. Parallel dazu sichert man die Daten zusätzlich in der Cloud, um im Falle eines Verschlüsselungsangriffs oder defekten Sicherungsmediums ebenfalls Zugriff auf die Daten zu haben. Der Nachteil der Cloud ist der langsamere Zugriff auf die Datensicherung, denn diese müssen ja dann erst einmal wieder alle aus der Cloud über das Internet zurückgespielt werden. Nachteil einer hybriden Sicherung sind zusätzliche einmalige und monatliche Kosten. Hier bleibt nur eine klare Abwägung von Risiko und potenziell verlorenen Daten. Die zusätzlichen Kosten für die Datensicherung muss man in dem Fall als eine Art „Versicherungsgebühr" ansetzen und dann entscheiden, ob man diese Versicherung braucht. Ergänzend bietet die Versicherungsbranche auch „Cyberschutzversicherungen" an, die als Teil des Risikomanagements Unternehmen gegen existenzgefährdende Folgen eines Cyber-Vorfalls wie beispielsweise Datenverlust und Datenschutzverletzung absichern sollen. Schutz bietet eine Cyberversicherung jedoch nur in finanzieller Hinsicht. Verlorene und/oder verschlüsselte Daten kann auch eine Versicherung nicht wieder zurückbringen und von Ihren Pflichten im Sinne von Datensicherung und Datenschutz entbindet eine solche Versicherung auch nicht. Daher ist auch hier eine Abwägung von Kosten und Nutzen individuell von der Golfanlage vorzunehmen.

Alternative „komplettes Arbeiten in der Cloud"

Immer mehr Anlagen verlegen ihren Server und somit ihre Daten komplett in die Cloud. Vorteil ist dabei, dass das gesamte Datensicherungsproblem gelöst ist. Nachteil ist die komplette Abhängigkeit vom Internet – denn ohne

6 https://de.wikipedia.org/wiki/Generationenprinzip

Internet gibt es dann auch keinen Zugriff auf den Server, die Programme und die Daten. Eine „Ausfallsicherung“ per Mobilfunk ist leider noch nicht bei allen Golfanlagen realisierbar, so dass diese Lösung leider noch nicht für alle Anlagen und Standorte verfügbar ist. Gerade wenn Neuinvestitionen in Server-Hardware anstehen, sollten Sie diese Alternative mit Ihrem IT-Betreuer einmal besprechen.

Einsparpotenziale für Gemeinnützige Gesellschaften/Vereine

Für gemeinnützige Vereine und Gesellschaften stellen einige Hersteller (u.a. Microsoft) stark vergünstigte bzw. teilweise kostenlose Lizenzen zur Verfügung (Stichwort: NON PROFIT), so dass auch hier z.B. mit Office 365 eine zusätzliche Möglichkeit besteht, eine zusätzliche Verfügbarkeit der Daten in der Cloud zu gewährleisten. Bei Microsoft stehen beispielsweise jedem zertifizierten NON PROFIT-Teilnehmer bis zu 10 kostenlose Office 365 PREMIUM-Lizenzen kostenlos (sog. Donation) zur Verfügung. Weitergehende Informationen zu den NON PROFIT-Programmen finden Sie im Web[7].

Fazit

Sprechen Sie mit Ihrem IT-Verantwortlichen und ggf. auch mit Ihrem Datenschützer über das individuelle Konzept Ihrer Golfanlage für den „Fall der Fälle“. Spielen Sie ggf. auch zusammen einmal die Situation durch. Damit die Funktionalität Ihrer Datensicherung auch langfristig erhalten bleibt, sollten Sie Ihren IT-Verantwortlichen auch mit einer dauerhaften Prüfung und ggf. auch einem Rücksicherungsversuch beauftragen und dokumentieren lassen.

Axel Heck

7 https://owncloud.pccaddie.net/index.php/s/d0jHZED5UFpiu0p